

Secure Sensitive Data (SSD) Properties op SX500 Series Stackable Switches

Doel

Secure Sensitive Data (SSD) Management wordt gebruikt om gevoelige gegevens zoals wachtwoorden en toetsen veilig op de switch te beheren. Deze informatie moet worden beveiligd wanneer deze van het ene apparaat naar het andere wordt verzonden. Het toegangsniveau van de gebruiker bepaalt hoe de gevoelige gegevens kunnen worden bekeken, als illustratie- of gecodeerde gegevens. SSD-eigenschappen zijn een verzameling parameters in combinatie met SSD-regels die instellingen controleren, zoals de versleuteling van gevoelige gegevens, de beveiliging van configuratiebestanden en de manier waarop de gevoelige gegevens in de huidige sessie worden bekeken.

Het doel van dit document is om te helpen bij de configuratie van Secure Sensitive Data (SSD) Properties op SX500 Series Stackable Switches.

Toepasselijke apparaten

- SX500 Series Stackable-switches

Softwareversie

- 1.3.0.62

SSD-eigenschappen

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > Secure Sensitive Data Management > Properties**. De pagina *Eigenschappen* wordt geopend:

Properties

Persistent Settings

Current Local Passphrase Type: Default

Configuration File Passphrase Control: Unrestricted
 Restricted

Configuration File Integrity Control: Enable

Current Session Settings

Read Mode: Plaintext
 Encrypted

Opmerking: Het veld Lokaal wachtwoord geeft het type lokaal wachtwoord dat oorspronkelijk is ingesteld weer.

Stap 2. Klik in het veld Wachtwoord voor configuratie van het bestand op de radioknop van het gewenste type wachtwoordcontrole. Bestandswachtwoord geeft extra bescherming aan het door de gebruiker ingestelde wachtwoord en de gegevens zijn versleuteld met het door de gebruiker ingestelde wachtwoord.

- Onbeperkt — Het door de gebruiker gedefinieerde wachtwoord is opgenomen in het configuratiebestand dat van het ene apparaat naar het andere wordt verzonden.
- Beperkt — Het door de gebruiker gedefinieerde wachtwoord is niet in het configuratiebestand opgenomen.

Stap 3. (Optioneel) Controleer de integriteitscontrole van het bestand door het vakje **Enable** in het veld Configuration File Integrity Control in te schakelen. Met deze optie voorkomt u dat het configuratiebestand wordt aangepast.

Stap 4. Klik in het veld Lezen op de gewenste radioknop. De beschikbare opties zijn:

- Plaintext — De gevoelige gegevens worden weergegeven in de vorm van een illustratie.
- Versleuteld — De gegevens worden versleuteld.

Stap 5. Klik op **Toepassen**.

Lokale wachtwoord wijzigen

Stap 1. Meld u aan bij het web configuratieprogramma en kies **Security > Secure Sensitive Data Management > Properties**. De pagina *Eigenschappen* wordt geopend:

Properties

Persistent Settings

Current Local Passphrase Type: Default

Configuration File Passphrase Control: Unrestricted
 Restricted

Configuration File Integrity Control: Enable

Current Session Settings

Read Mode: Plaintext
 Encrypted

Apply Cancel **Change Local Passphrase**

Stap 2. Klik op **Lokaal wachtwoord wijzigen** om het huidige lokale wachtwoord te wijzigen. De pagina *Lokale wachtwoord wijzigen* wordt geopend:

Change Local Passphrase

The minimum requirements for Local Passphrase are as follows:

- Should be at least 8 characters up to 16 characters.
- Should be at least one upper case character, one lower case character, one numeric number, and one special character e.g. #,\$.

Current Local Passphrase Type: Default

Local Passphrase: Default
 User Defined (Plaintext) (0/16 Characters Used)

Confirm Passphrase

Apply Cancel Back

Opmerking: Het veld Lokaal wachtwoord wordt weergegeven in het veld Lokaal wachtwoord.

Change Local Passphrase

The minimum requirements for Local Passphrase are as follows:

- Should be at least 8 characters up to 16 characters.
- Should be at least one upper case character, one lower case character, one numeric number, and one special character e.g. #,\$.

Current Local Passphrase Type: Default

Local Passphrase: Default
 User Defined (Plaintext) (10/16 Characters Used)

Confirm Passphrase

Apply Cancel Back

Stap 3. Klik in het veld Lokale wachtwoord op de radioknop van het gewenste lokale wachtwoord:

- Standaard: dit is de standaardwachtwoord.
- Gebruikershandleiding (Plaintext) — Voer het gewenste wachtwoord in. Het moet tussen 8 en 16 tekens bevatten, hoofdletters en kleine letters, een nummer en een speciaal teken.
- Wachtwoord bevestigen — Voer het door de gebruiker gedefinieerde wachtwoord

opnieuw in.

Stap 4. Klik op **Toepassen**.